UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

In re Flagstar December 2021 Data Security Incident Litigation	Case No. 4:22-cv-11385 Hon. Brandy R. McMillion Magistrate Judge Kimberly G. Altman **REPLY BRIEF IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS THE CONSOLIDATED CLASS ACTION COMPLAINT**

William E. Ridgway
Marcella Lape
Lindsey Sieling
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
155 N. Wacker Dr., Suite 2700
Chicago, IL 60606
Telephone: (312) 407-0700
William.Ridgway@skadden.com
Marcie.Lape@skadden.com
Lindsey.Sieling@skadden.com

Sean P. McNally (P66292)
Jason E. Manning
TROUTMAN PEPPER HAMILTON SANDERS LLP
4000 Town Center, Suite 1800
Southfield, MI 48075
Telephone: (248) 359-7300
Sean.McNally@troutman.com
Jason.Manning@troutman.com

Counsel for Defendant

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

REGULATIONS

PRELIMINARY STATEMENT

Defendants demonstrated in their Opening Memorandum that Plaintiffs not only failed to allege a concrete injury fairly traceable to the Cyber Incident[1] but, as a factual matter, they could not meet their burden of establishing Article III standing because the Cyber Incident involved no exposure of data on the dark web and could not result in the alleged injuries to Plaintiffs. Instead of immediately responding, Plaintiffs tried to salvage their case through discovery. For over five months, Plaintiffs searched for evidence to support their unsupported allegations. But Plaintiffs emerged from that process empty handed. When they finally filed their Opposition, Plaintiffs did not offer a shred of evidence that any Plaintiff suffered a concrete harm traceable to the Cyber Incident. Nor did they produce a single affidavit from an expert or Plaintiff that even attempted to connect the claimed injuries to the Cyber Incident. Instead, Plaintiffs tried to distract the Court by harping on claimed gaps in Flagstar's evidence. But that reverses the burden. It is *Plaintiff*s who need to establish subject matter jurisdiction. Because they have failed to do so, the Court should dismiss the Consolidated Complaint in full.

Moreover, even if the Plaintiffs could demonstrate Article III standing, Plaintiffs' claims suffer from numerous pleading deficiencies and would nonetheless be subject to dismissal under Rule 12(b)(6).

[1] Capitalized terms are defined in Defendants' opening brief, ECF No. 58.

ARGUMENT[2]

I. PLAINTIFFS LACK STANDING UNDER ARTICLE III.

Plaintiffs essentially ask this Court to allow the case to go forward based on the fact of the data breach alone. But as case law makes clear, many cyber incidents do not result in a concrete injury and Article III standing. This case is yet another example.

A. Plaintiffs Fail to Plausibly Allege a Cognizable Injury That Is Traceable to the Cyber Incident.

Although Plaintiffs' Opposition largely focuses on Flagstar's factual challenge to standing, the Court need not even consider the factual challenge because Plaintiffs' Complaint fails on its face: Plaintiffs do not even *allege* plausible cognizable injuries that are fairly traceable to the Cyber Incident.

It is undisputed that Plaintiffs allege no details connecting the purported misuse of certain Plaintiffs' PII to the Cyber Incident; nothing in Plaintiffs' Opposition argues otherwise. Plaintiffs instead suggest they can meet their burden simply by alleging that criminals stole their PII—though they do not specifically allege *what* PII was stolen for each Plaintiff—and that their injuries "were a result of the data breach." ECF No. 72, PageID.1511-12. Conclusory allegations like that are not enough to survive a facial challenge and establish that an injury is traceable

[2] For the Court's reference, attached as Exhibit 1 is a chart summarizing the reasons that Plaintiffs' claims should be dismissed.

to a data breach. As one court recognized, "[g]iven the frequency of data breaches and credit card fraud, and considering how many entities potentially come into possession of one's credit card information . . . any enterprising plaintiff could allege they experienced a fraudulent charge and attempt to connect it to any breach." *Smith v. Sabre Corp.*, 2017 WL 11678765, at *4 (C.D. Cal. Oct. 23, 2017) (no "logical connection" between data breach and fraudulent charges); *see also McCombs v. Delta Grp. Elecs., Inc.*, 2023 WL 3934666, at *6 (D. N.M. June 9, 2023).[3] This is precisely what Plaintiffs attempt to do here.[4]

Given the prevalence of data breaches, Plaintiffs are also wrong to suggest that the issue of whether Plaintiffs' PII may have been compromised in other security incidents has no bearing on standing. ECF No. 80, PageID.1309. Here, Plaintiffs do not allege that the PII that was purportedly misused was even compromised in the Cyber Incident. The cases Plaintiffs rely on are therefore

[3] While Plaintiffs try to distinguish *McCombs*, that case involved allegations very similar to here. The plaintiff alleged unauthorized attempts to access her bank account and a purported increase in spam communications following a breach that impacted names, Social Security numbers, and financial account numbers. 2023 WL 3934666, at *6. The Court concluded, however, that the plaintiff had not sufficiently alleged a causal connection and thus lacked Article III standing. *Id.*

[4] The cases Plaintiffs cite involved more detailed allegations than here. For example, in *In re SuperValu, Inc.*, 870 F.3d 763 (8th Cir. 2017), the one plaintiff who alleged a fraudulent charge on his credit card alleged that he had used the same credit card at the defendant's store shortly before the breach. *Id.* at 767, 772. No such details are offered here. And notably, the court affirmed the dismissal for lack of standing of the fifteen plaintiffs who alleged no misuse. *Id.* at 774.

inapposite as they involved the purported misuse of credit card and bank account information that *was* alleged to have been compromised in the breach at issue. Thus, the fact that the same credit card and bank account data could also have been compromised in a different data breach was not sufficient to defeat standing at the motion to dismiss stage. That is not the case here.

Once Plaintiffs' insufficient allegations of misuse of PII are stripped away, all that remains is the alleged risk of future harm, coupled with other non-cognizable injuries.[5]

Future Risk of Identity Theft or Fraud. Plaintiffs argue that they satisfy standing because the purported misuse of certain Plaintiffs' PII results in their risk of identity theft being sufficiently "imminent." ECF No. 72, PageID.1503-04. But without plausible allegations of misuse in the last *two years* traceable to the Cyber Incident, the risk of future harm is neither imminent nor substantial.[6] And even if Plaintiffs plausibly alleged an imminent risk of future harm, that would still not be sufficient to plead standing in a suit for damages, as the Supreme Court recognized in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021). *Id.* at 2210-11. Plaintiffs' reliance on the Sixth Circuit's pre-*TransUnion*, unpublished decision in *Galaria v.*

[5] Even if some Plaintiffs have plausibly alleged misuse traceable to the breach, which they have not, that is insufficient to confer standing on other Plaintiffs who have not alleged any misuse. *See In re Supervalu, Inc.*, 870 F.3d at 769-72.

[6] Plaintiffs largely rely on pre-*TransUnion* cases, or cases involving plausible allegations of misuse of PII, making them distinguishable from the case here.

Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016), is misplaced. Indeed, courts in the Sixth Circuit have recognized that *TransUnion* "casts some doubt on the continued viability of *Galaria*." *Brickman v. Maximus, Inc.*, 2022 WL 16836186, at *3 (S.D. Oh. May 2, 2022); *see also Kingen v. Warner Norcross + Judd LLP*, 2023 WL 8544231, at *2 (W.D. Mich. Oct. 4, 2023) ("*TransUnion* seems to reign in *Galaria's* future substantial risk of injury standard.").[7]

***Mitigation Costs*.** Plaintiffs acknowledge that mitigation costs qualify as a "concrete injury" only when there is a "substantial risk of harm," ECF No. 72, PageID.1506, which, as discussed above, is not present here.

***Lost Value of PII*.** Plaintiffs rely primarily on *In re Marriott International, Inc., Customer Data Security Breach Litigation* to argue that lost value of PII is a cognizable injury. ECF No. 72, PageID.1507-08. But *Marriott* involved plausible allegations of misuse that caused plaintiffs to "suffer[] lower credit scores[,]" not present here. 440 F. Supp. 3d 447, 462 (D. Md. 2020); *see also Stamat v. Grandizio Wilkins Little & Matthews, LLP*, 2022 WL 3919685, at *7 (D. Md. Aug. 31, 2022) (misuse of PII can lower credit scores but until that occurs, one "has not been concretely harmed").

[7] The court in *Kingen* has certified its order denying defendant's 12(b)(1) motion to dismiss, and defendant has filed an interlocutory appeal, meaning that the Sixth Circuit will likely address the viability of *Galaria* post-*TransUnion*. *Kingen*, No. 1:22-cv-01126-PLM-RSK, ECF Nos. 55-56.

Loss of Privacy. Plaintiffs do not allege any "emotional distress, anxiety, [or] increased concerns" stemming from the purported loss of privacy as they claim in their Opposition. ECF No. 72, PageID.1508. But even if they did, anxiety or emotional distress—which must be "severe"—is not a cognizable injury where, as here, "it is merely a fear of a future harm that is not 'certainly impending.'" *Garland v. Orlans, PC*, 999 F.3d 432, 440 (6th Cir. 2021).

Benefit of the Bargain. A "majority of courts have found that similar allegations of loss of bargained-for services in data breach cases are not sufficiently concrete to satisfy the injury in fact requirement of Article III standing." *Duqum v. Scottrade, Inc.*, 2016 WL 3683001, at *6 (E.D. Mo. July 12, 2016) (citation omitted); *see also Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 754-55 (W.D.N.Y. 2017). That is particularly true here, where Plaintiffs do not allege what money, if any, they paid for Flagstar's services.[8]

B. Plaintiffs Offer No Evidence Establishing Article III Standing.

Even if Plaintiffs' threadbare allegations would otherwise be sufficient to plead an injury traceable to the Cyber Incident, in its Motion to Dismiss, Flagstar challenged the factual basis for those allegations and submitted evidence showing

[8] Plaintiffs are also wrong that purported spam communications support standing. ECF No. 80, PageID.1511. As Defendants' authority recognizes, "[c]ourts have generally rejected the theory that unsolicited calls or emails constitute an injury in fact" that is traceable to a data breach. *Cooper v. Bonobos, Inc.*, 2022 WL 170622, at *5 (S.D.N.Y. Jan. 19, 2022); *see also* ECF No. 58, PageID.698-99.

that (1) Flagstar paid a $1 million ransom in exchange for, among other things, the deletion of the data exfiltrated in the Cyber Incident and an agreement not to post the data anywhere, (2) Flagstar's vendor deleted Flagstar's data from the threat actor's server, (3) Flagstar has found no evidence that any of the data from the Cyber Incident has been released on the dark web, (4) for several plaintiffs, the purported PII they claim was misused was not compromised in the Cyber Incident, and (5) at least seven plaintiffs have had their PII disclosed in other data breaches. ECF No. 58, PageID.690, 692-93, 699-700.

In response, Plaintiffs failed to offer *any* affirmative evidence of their own establishing cognizable injuries traceable to the Cyber Incident. Instead, they relied exclusively on their unsupported allegations in the Complaint and attempted to "point[] to alleged weaknesses" in Flagstar's evidence. *De Angelis v. Nat'l Ent. Grp., LLC*, 2018 WL 11316612, at *5 (S.D. Ohio July 25, 2018). But Plaintiffs "cannot meet [their] burden of proving standing without pointing to any evidence of [their] own." *Id.* at *6; *see also* ECF No. 58, PageID.694-95. When a factual challenge is made, there is "no presumptive truthfulness . . . to the factual allegations." *Ohio Nat. Life Ins. Co. v. U.S.*, 922 F.2d 320, 325 (6th Cir. 1990). Rather, the trial court must "weigh the evidence" and "the plaintiff will have the burden of proof that jurisdiction does in fact exist." *RMI Titanium Co. v. Westinghouse Elec. Corp.*, 78 F.3d 1125, 1134 (6th Cir. 1996). Nor, as shown

below, can Plaintiffs sidestep their burden by asserting that the factual challenge is a premature attack on the merits or that it cannot be resolved because there are disputed issues of fact.

1. The Factual Challenge to Standing is Not a Premature Attack on the Merits.

First, Plaintiffs are wrong that the Court should ignore the factual challenge to standing because doing so "implicate[s] the merits" of their claims. ECF No. 72, PageID.1513 (quoting *Gentek Bldg. Prods. Inc. v. Sherwin-Williams Co.*, 491 F.3d 320, 330-31 (6th Cir. 2007)). The Sixth Circuit case that Plaintiffs rely on, *Gentek*, addressed a factual challenge to *federal question* jurisdiction, and the Court concluded that a factual challenge that implicates an element of a *federal* claim that provides the basis of jurisdiction should generally not be resolved at the motion to dismiss stage. 491 F. 3d at 330. Yet as Judge Levy recently observed (which Plaintiffs neglect to mention), *Gentek*'s general rule does not apply where, as here, the factual challenge is to Article III standing and "[p]laintiffs' claims are all state law claims, and the Class Action Fairness Act . . . is the basis for the Court's jurisdiction." *Myslivecek v. FCA US LLC*, 2022 WL 17904526, at *7 (E.D. Mich. Dec. 23, 2022) ("Unlike in *Gentek*, the factual dispute [on Article III standing] does not go to an element of a federal statute providing the court with

jurisdiction.").[9]

Numerous courts in other data breach cases have dismissed complaints following a factual challenge to Article III standing where, as here, plaintiffs fail to present evidence tying their purported injuries to the data breach. *See, e.g.*, *Masterson v. IMA Financial Grp., Inc.*, 2023 WL 8647157, at *5 (D. Kan. Dec. 14, 2023); *Shepherd v. Cancer & Hematology Ctrs. of W. Mich., P.C.*, 2023 WL 4056342, at *7 (W.D. Mich. Feb. 28, 2023); *Patterson v. Med. Rev. Inst. of Am.*, 2022 WL 2267673, at *3 (N.D. Cal. June 23, 2022); *Burns v. Mammoth Media, Inc.*, 2021 WL 3500964, at *4 (C.D. Cal. Aug. 6, 2021); *Foster v. Essex Prop., Inc.*, 2017 WL 264390 (N.D. Cal. Jan. 20, 2017).

The out-of-circuit data breach cases Plaintiffs point to are inapt because, unlike here, the courts were addressing the factual challenge without any discovery. *See, e.g.*, *In re Blackbaud, Inc., Customer Data Breach Litig.*, 2021 WL 2718439 (D.S.C. July 1, 2021) (noting that it was "premature to dismiss Plaintiffs' claims on grounds of traceability" when there had been no discovery); *In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183,

[9] *See also De Angelis*, 2018 WL 11316612, at *4 ("In cases finding that the standing question is inextricably intertwined with the merits, standing often turns on the interpretation of the language in the statute that is the basis for federal question jurisdiction."); *In re Foreclosure Cases*, 2007 WL 4589765, at *3 (S.D. Ohio Dec. 27, 2007) (resolving 12(b)(1) factual challenge to standing and distinguishing *Gentek* because "[p]laintiffs' cause of action is created by state law, not a federal statute, and jurisdiction is based on diversity, not a federal question").

1206-07 (S.D. Fla. May 10, 2022) (court was not prepared to find that plaintiffs lacked standing "without the aid of discovery" and where plaintiffs provided an expert declaration that contradicted some of defendants' findings). Here, Plaintiffs spent over five months pursuing jurisdictional discovery. Plaintiffs received documents not only from Flagstar, but also from two third parties—Tetra Defense (n/k/a Arctic Wolf), the vendor that negotiated the ransom and deleted the data, and Kroll, the vendor that investigated the incident. Plaintiffs also scheduled a 30(b)(6) deposition of Tetra Defense but canceled that deposition less than a week before it was set to occur. *See* Ex. 2, Jan. 26, 2024 email. Because their discovery yielded no evidence of a traceable injury, Plaintiffs now change their tune and claim the issue is premature. But deferring the issue is unfair to Defendants—who have spent five months on discovery regarding an issue that Plaintiffs now claim is premature—and will only serve to waste the Court's and the Parties' resources.

2. There Are No Material, Disputed Facts.

Nor are there material, disputed facts that prevent the Court from ruling on Flagstar's factual challenge to standing. Plaintiffs have not produced a single piece of evidence in support of their jurisdictional allegations, and on a factual challenge, there is "no presumptive truthfulness . . . to the factual allegations." *Ohio Nat. Life Ins.*, 922 F.2d at 325. And even if Plaintiffs had produced evidence that created a material factual dispute, the Court is "empowered to resolve factual disputes" to

determine whether subject matter jurisdiction does or does not exist. *RMI Titanium*, 78 F.3d at 1134 (distinguishing Rule 12(b)(1) factual challenge to subject matter jurisdiction from Rule 56 motion for summary judgment).

Rather than present evidence, Plaintiffs attempt to shift the burden to Flagstar, arguing that Flagstar has not offered competent evidence establishing "what data was stolen and when, who stole it, and what those actors might have done with it during, and for the months following, the breach." ECF No. 72, PageID.1515. But Flagstar does not have the burden to *disprove* standing; Plaintiffs have the burden to prove it. *See Cartwright v. Garner*, 751 F.3d 752, 760 (6th Cir. 2014). Plaintiffs' attempt to undermine the evidence that Flagstar produced gets them nowhere: Plaintiffs cannot create a material dispute of fact where they have relied on allegations alone.

First, Plaintiffs mischaracterize Ms. Charters' declaration and testimony and falsely claim that she lacks personal knowledge of the ransom negotiations and data deletion. ECF No. 72, PageID.1490, 1515. Ms. Charters (Flagstar's Chief Information Officer) testified that she was involved in Flagstar's response to the Cyber Incident, including through regular executive team meetings. ECF No. 72-2, PageID.1572-73, 1583-84 (Charters Dep. at 33:14-34:22, 44:10-16, 45:2-13). While Ms. Charters may not have personally communicated with the threat actor, paid the ransom, or deleted the data, she knew about those activities in real-time

through executive meetings and her review of materials shared during those meetings. *Id.* at PageID.1583-84, 1591-93, 1604-05 (Charters Dep. at 44:10-16, 45:9-13, 52:14-16, 53:22-54:4, 65:23-66:6). Ms. Charters also testified that before signing her declaration, she considered—in addition to the lists of impacted individuals—her "recollection of the events that [she] participated in related to the incident that was described." *Id.* at PageID.1566 (Charters Dep. at 27:8-14).[10]

Flagstar, moreover, produced other competent evidence showing that the threat actor agreed to allow Flagstar to delete the data from the threat actor's server in exchange for a ransom payment of $1 million, the ransom was paid, and the data was deleted. *See* ECF No. 72.05 (threat actor communications, filed under seal) at FLAG-DEC-0000032 (documenting agreement); *id.* at FLAG-DEC-00000033 (Bitcoin payment); *id.* at FLAG-DEC-0000017 (deletion of data). And Plaintiffs also had the opportunity to take the deposition of a corporate representative from Tetra Defense, Nathan Little, who was personally involved in the ransom negotiations and data deletion, but chose to cancel that deposition less than a week before it was scheduled to occur. Ex. 2, Jan. 26, 2024 email. This Court should not reward Plaintiffs' strategic decision to forgo pursuing this evidence and accept their unsupported speculation that the threat actor may have retained data.

[10] Ms. Charters also confirmed that there was nothing in her declaration that she needed to amend or change. *Id.* at PageID.1566-67 (Charters Dep. at 27:23-28:1).

Second, Plaintiffs argue that Flagstar has not submitted evidence proving that the stolen data was not made available on the dark web for ten months after the breach, ECF No. 72, PageID.1515, but that is untrue. Moreover, it is Plaintiffs' burden to present evidence that the data from the Cyber Incident *was available* on the dark web, and they have not done so. In addition to the affidavit of Ms. Charters, Plaintiffs ignore other evidence, including that Flagstar engaged Tetra Defense on December 13, 2021, to (among other things) monitor the dark web.[11] Mr. Hardin also testified that he has been involved in thousands of ransomware cases and has facilitated thousands of ransom payments, and in his experience, stolen data has *never* been posted to the dark web following the payment of a ransom. *See* Ex. 4, Hardin Dep. 125:4-126:6.[12] While Plaintiffs criticize the thoroughness of Mr. Hardin's dark web search, ECF No. 72, PageID.1499-501, Plaintiffs have apparently not been able to locate the data on the dark web either, or they certainly would have cited to that evidence in their Opposition. Plaintiffs cannot meet their burden by relying on mere speculation that the data *could* have

[11] Ex. 3 at 1, Tetra Defense Statement of Work ("Objectives: . . . Monitor dark web data breach sites for posting of Client name or data"); *id.* at 2 ("Monitor all known data leak sites for any publication of Client's name and/or data" and "Monitor general Dark Web forums for any publication of Client's name and/or data.").

[12] *See also id.* at 132:5-7 ("In my opinion, based off all the cases I've worked on, when payment has been made, information has not been leaked."); *id.* at 137:23-25 ("In the cases that I have handled and the payments that . . . have been made, the data of my clients has not been leaked out on the Dark Web.").

been posted to the dark web at some point.

Third, Plaintiffs complain that Ms. Charters did not personally prepare the master lists of individuals impacted in the incidents. But Ms. Charters testified that members of Flagstar's data analytics team within the IT organization, which Ms. Charters manages,[13] prepared the lists and that she reviewed those lists prior to signing her declaration to confirm the facts set forth therein.[14] Plaintiffs, moreover, offer no evidence contradicting those paragraphs of Ms. Charters' declaration.

Finally, while Plaintiffs claim that Ms. Charters does not have personal knowledge of whether the compromised data from the Accellion breach is available on the dark web, Plaintiffs do not actually dispute that fact. Nor could they, given that Plaintiffs' own counsel has pointed to the presence of this data on the dark web in their complaint against Flagstar relating to the Accellion breach. *See* Third Consolidated Class Action Compl. ¶¶ 6, 8, *Angus v. Flagstar Bank, N.A.*, No. 2:21-cv-10657-MFL-DRG, ECF No. 69, PageID.1064-65 (E.D. Mich. filed Sept. 12, 2023). This is not "irrelevant" to standing as Plaintiffs claim, particularly when Plaintiffs produce no evidence showing that their purported injuries are

[13] ECF No. 72-2, PageID.1556-57, 1565 (Charters Dep. at 17:12-18:11, 26:3-12).

[14] Plaintiffs claim that Ms. Charters reviewed "excerpts" of the lists. ECF No. 72, PageID.1516. In fact, Ms. Charters reviewed the master lists prior to signing her declaration. *See* ECF No. 72-2, PageID.1631 (Charters Dep. at 92:2-10). The "excerpts" were taken from those master lists and produced to Plaintiffs in response to their discovery requests.

traceable to the Cyber Incident.

In short, the attack on Ms. Charters is misplaced and irrelevant because Plaintiffs have not offered any evidence to support the allegations in their Complaint, and that fact cannot be disputed. Plaintiffs have thus failed to meet their burden of presenting evidence establishing a cognizable injury traceable to the Cyber Incident, and therefore dismissal of the Complaint is warranted.[15]

II. The Complaint Should Be Dismissed Under Rule 12(b)(6).

A. Choice of Law for Common Law Claims.

Plaintiffs do not take a position on which state's laws should apply to their claims but contend that it is a fact-intensive inquiry that should not be resolved before discovery. ECF No. 72, PageID.1517. Yet courts routinely resolve choice-of-law issues at the motion to dismiss stage, particularly where, as here, "the relevant facts are sufficiently clear that delay in making a choice-of-law determination would serve no useful purpose." *Foisie v. Worcester Polytechnic Inst.*, 967 F.3d 27, 42 (1st Cir. 2020). Michigan is where Flagstar is headquartered and where Plaintiffs allege a "substantial part of the conduct giving rise to Plaintiffs' claims occurred." ECF No. 52, PageID.546. Thus, Michigan law should

[15] If the Court believes there are disputed facts that are "essential" to the determination of standing—notwithstanding Plaintiffs' failure to present any affirmative evidence of their own—the proper course is to hold an "evidentiary hearing" where the Court can consider and weigh the evidence presented by both parties. *Bischoff v. Osceola Cty., Fla.*, 222 F.3d 874, 879 (11th Cir. 2000).

apply. *See Hummel v. Teijin Auto. Tech., Inc.*, 2023 WL 6149059, at *4 (E.D. Mich. Sept. 20, 2023) (applying Michigan law in data breach class action).

B. Plaintiffs' Negligence Claim Fails.

The negligence claim fails for multiple, independent reasons. *First*, Plaintiffs claim that they "do not seek to hold Flagstar liable 'for the fact of the data breach alone,'" ECF No. 72, PageID.1519 (quoting *In re Waste Mgmt.*, 2022 WL 561734, at *7 (S.D.N.Y. Feb. 24, 2022), but that is precisely what they are attempting to do. "[T]he law does not impose strict liability for harms arising out of the storage of personal information," *In re Waste Mgmt.*, 2022 WL 561734, at *5, and Plaintiffs must do more than make the conclusory allegation that Flagstar "fail[ed] to comply with state and federal law and industry standards," ECF No. 72, PageID.1518, to state a claim. *See Ashcroft v. Iqbal, 556 U.S. 662*, 679 (2009) (courts "are not bound to accept as true a legal conclusion couched as a factual allegation").[16]

Second, Plaintiffs attempt to distinguish *Rakyta v. Munson Healthcare*, 2021 WL 4808339 (Mich. Ct. App. Oct. 14, 2021) and *Doe v. Henry Ford Health Sys.*,

[16] Plaintiffs do not dispute that negligence *per se* is not an independent cause of action in Michigan. *See* ECF No. 72, PageID.1518-21. Count two should therefore be dismissed. To the extent Plaintiffs allege violations of the FTC Act or the GLBA to establish the duty and breach elements of a negligence claim, their negligence claim still fails because Plaintiffs do not allege a specific duty imposed by the FTC Act or GLBA, *see In re Brinker Data Incident Litig.*, 2020 WL 691848, at *9 (M.D. Fla. Jan. 27, 2020), or allege with any specificity how Flagstar breached any duty imposed by the FTC Act or GLBA.

308 Mich. App. 592 (Ct. App. Dec. 18, 2014)—two Michigan data breach cases directly on point—because they did not involve any allegations of misuse of PII. But that is precisely the case with Plaintiffs Kennedy, Tallman, Wiedder, McCarthy, Hernandez, Worton, Turner, and McLaughlin—there are no allegations of misuse of their PII. The fact that *other* Plaintiffs have alleged misuse (albeit not traceable to the Cyber Incident) does not transform these Plaintiffs' potential *future* injuries into *present* ones. *See Rakyta*, 2021 WL 4808339, at *4 ("An injury that is imminent is an injury that has not yet occurred.").

Third, Plaintiffs do not dispute that they must allege both a temporal and logical relationship between the purported misuse of certain Plaintiffs' PII and the Cyber Incident. *See* ECF No. 72, PageID.1521. Yet Plaintiffs ignore completely the types of allegations that courts consider when determining whether a logical causal relationship is pled. *Galaria v. Nationwide Mut. Ins. Co.*, 2017 WL 4987663, at *7 (S.D. Ohio Aug. 16, 2017). Instead, Plaintiffs cite to temporal allegations in the Complaint and cases where courts rely on injuries not cognizable under Michigan law to establish causation. *See* ECF No. 72, PageID.1521.

C. Plaintiffs' Breach of Confidence Claim Fails.

Plaintiffs cite no applicable authority for the proposition that Michigan recognizes a standalone breach of confidence claim outside the trade secrets context. Indeed, *Eickenroth v. Roosen, Varchetti & Olivier, PLLC*, 2021 WL

1224912 (E.D. Mich. Mar. 31, 2021), involved claims under the Fair Debt Collections Practices Act, not a standalone claim for breach of confidence.[17] The other cases cited by Plaintiffs are also inapposite, involving claims under other states' laws and/or allegations of intentional disclosure.

D. Plaintiffs' Invasion of Privacy Claim Fails.

Plaintiffs do not dispute that under Michigan law an intrusion upon seclusion claim focuses on the way information was obtained by the defendant, not its publication. *See* ECF No. 72 PageID.1523. Instead, Plaintiffs contend that Flagstar's alleged knowing failure to address unidentified vulnerabilities constitutes an intentional disclosure to the cybercriminals responsible for the Cyber Incident. *Id.* These allegations are not sufficient to state a claim for negligence, *see* Section II.B.1, let alone an intentional invasion of privacy.[18]

E. Plaintiffs' Breach of Contract Claims Fail.

The breach of contract claims fail for multiple reasons. *First*, there is no

[17] *See also State Farm Mut. Auto. Ins. Co. v. Elite Health Ctrs., Inc.*, 2019 WL 2576360, at *3 (E.D. Mich. June 24, 2019) (considering whether to exclude evidence purportedly obtained as a result of a law firm's alleged disclosure of client confidences); *Richard v. Detroit Tr. Co.*, 269 Mich. 411 (1934) (considering whether to declare a contract null and void).

[18] Plaintiffs' cases, all of which apply other states' invasion of privacy laws, are inapposite or involve intentional conduct. *See, e.g.*, *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 819 (E.D. Ky. 2019) ("Plaintiffs allege that an employee of [defendant] took an affirmative action to gather the tax information…and send it in response to a fraudulent email.").

express or implied contract here. As for their express contract claim, Plaintiffs do not explain how it is plausible that the quoted privacy policies, which do not even pre-date the Cyber Incident, could constitute an enforceable contract, particularly when Plaintiffs do not allege that they even read those policies. Plaintiffs claim such an allegation is unnecessary because Michigan courts follow the objective theory of assent. ECF No. 72, PageID.1525. But a reasonable person in the position of Plaintiffs—who have not read the privacy policy—could not possibly understand it to be an enforceable contract. *Rood v. Gen. Dynamics Corp.*, 507 N.W.2d 591, 601 (Mich. 1993) (informal policy did not provide support for mutual assent where "[t]he record does not indicate that [plaintiff] was even aware of this policy"). And even if Plaintiffs had read the privacy policy, it disclaims any such interpretation.[19] Courts have found similar allegations to be insufficient to state a claim. *See, e.g.*, *Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010) (dismissing breach of contract claim where plaintiffs did not read the documents on which the claim was based).[20]

---

[19] *See* https://www.flagstar.com/legal-disclaimers/privacy-statement.html (last visited Mar. 18, 2024) ("While we are focused on the security of your Personal Information, you must remember that the Internet is a global communications vehicle open to threats, viruses, and intrusions from others. For this reason, Flagstar cannot promise, and you should not expect, that we will be able to protect your Personal Information at all times and in all circumstances.").

[20] The cases cited by Plaintiffs are distinguishable. ECF No. 72, PageID.1524. In two of the cases, the parties entered into express contracts that incorporated

(cont'd)

Plaintiffs' implied contract claim fares no better. In their Opposition, Plaintiffs largely rely on cases where an implied contract was found in the employment context, like *Hummel* and *Enslin*. *See* ECF No. 72, PageID.1527-28. But those cases are distinguishable because here, the implied contract claim is brought on behalf of Flagstar's current and former *customers*, whose conduct differs from employees. *See* Compl. ¶¶ 6-19, PageID.547-56.

Second, Plaintiffs are wrong that Michigan's statute of frauds does not apply because the federal regulation is for an indefinite term. ECF No. 72, PageID.1526. Plaintiffs rely on a case addressing at-will employment contracts, which can last for two days, two years, or more. In contrast, Flagstar must maintain customers' PII for at minimum five years. *See* 31 C.F.R. § 1020.220(a)(3)(ii). The purported contract to "safeguard" Plaintiffs' PII thus cannot be completed within one year, bringing it squarely within Michigan's statute of frauds.

Finally, as discussed above, Plaintiffs allege no credible damages caused by such breach. *See supra* Section II.B. Plaintiffs are wrong that they need not allege actual damages because Michigan law infers nominal damages from a breach of contract. ECF No. 72, PageID.1526-27. Plaintiffs ignore two data breach cases

---

defendants' relevant privacy policies. *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735 (W.D.N.Y. 2017), *on reconsideration*, 304 F. Supp. 3d 333 (W.D.N.Y. 2018); *Huong Hoang v. Amazon.com, Inc.*, 2012 WL 1088165 (W.D. Wash. Mar. 30, 2012). In *Marriott*, the plaintiffs sufficiently alleged an offer and acceptance that occurred *prior* to the data breach. 440 F. Supp. 3d at 484.

where the Michigan Court of Appeals affirmed the dismissal of breach of contract claims for failure to plead damages. *Doe*, 308 Mich. App. at 603 ("[D]amages are not presumed in relation to contracts . . . ."); *Rakyta*, 2021 WL 4808339, at *7.

F. Plaintiffs' Unjust Enrichment Claim Fails.

Plaintiffs' unjust enrichment claim fails for the same reason its benefit-of-the-bargain theory of standing fails—to the extent Plaintiffs paid any money to Flagstar (which they do not specifically allege) they received financial services in exchange. *See* ECF No. 58, PageID.722-23; *In re Supervalu, Inc.*, 925 F.3d 955, 966 (8th Cir. 2019) ("[Plaintiff] paid for groceries . . . . He did not pay a premium 'for a side order of data security and protection.'" (citation omitted)). In addition, Plaintiffs continue to fail to allege that Flagstar received any benefit from Plaintiffs—Flagstar is required by federal law to obtain certain PII (including name, address, date of birth, and SSN) from customers prior to opening an account. *See* 31 CFR § 1020.220(a)(2)(i).

G. Plaintiffs' Declaratory Judgment Claim Fails.

The declaratory judgment claim should be dismissed because declaratory judgment is a form of relief, not an independent cause of action. Moreover, Plaintiffs have not alleged facts showing that another data breach is certainly impending and therefore lack standing. *See Lochridge v. Quality Temp. Servs.*,

Inc., 2023 WL 4303577, at *8 (E.D. Mich. June 30, 2023).[21]

H. Plaintiffs' Statutory Claims Fail.

1. The California Consumer Privacy Act Claim Fails.

First, Plaintiffs are wrong that "no more is required" of them than to allege the "specific ways that Flagstar's security measures caused them harm." ECF No. 72, PageID.1535. Plaintiffs must plausibly allege that their PII was stolen "as a result of the business's violation of the duty to implement and maintain *reasonable* security procedures and practices." Cal. Civ. Code § 1798.150(a)(1) (emphasis added). As discussed in Section II.B.1, Plaintiffs have pled nothing more than conclusory allegations that Flagstar's security practices were unreasonable.

Second, while Plaintiffs attack *Griffey v. Magellan Health Inc.*, 2022 WL 1811165 (D. Az. June 2, 2022) for relying on analogous California law to interpret the notice requirements of the CCPA, none of the cases Plaintiffs cite even *mentions* the CCPA, let alone discusses its notice requirements. *See* ECF No. 72, PageID.1536-37. Plaintiffs' reliance on CLRA cases, like *Morgan v. AT&T Wireless Servs., Inc.*, is misplaced given that the statute "contemplates that a

[21] Unlike *Finesse Express, LLC v. Total Quality Logistics, LLC*, 2021 WL 1192521 (S.D. Ohio Mar. 30, 2021), Plaintiffs do not allege that a declaratory judgment claim would clarify the parties' prospective obligations under the provisions of an express contract. Additionally, courts have declined to follow *Home Depot*. *See, e.g.*, *In re Brinker Data Incident Litig.*, 2020 WL 691848, at *11-12; *Collins v. Athens Orthopedic Clinic*, 356 Ga.App. 776, 849 S.E.2d 213, 218 n.8 (2020).

consumer may amend a complaint for injunctive relief to add a request for damages under the CLRA" after providing notice, unlike the CCPA. 177 Cal. App. 4th 1235, 1260 (2009).

2. No Claim for Violation of State Disclosure Laws.

California and Washington Plaintiffs' argument that they have adequately pled "incremental harm" from alleged delayed disclosure is belied by the Complaint. Not a single California or Washington Plaintiff alleges an injury that could have been mitigated by earlier disclosure. Plaintiffs next argue that whether Flagstar reasonably waited to notify customers is a question of fact. But courts have dismissed CCRA and similar claims based on equally deficient allegations. *See, e.g.*, *Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 56 (2021).

3. No Claim for Violation of State Consumer Fraud and Unfair and Deceptive Acts and Practices Laws.

Plaintiffs' consumer protection claims fail for various reasons. *First*, Plaintiffs Kennedy, Tallman, Wiedder, McCarthy, Worton, McLaughlin, and Smith fail to allege cognizable injuries under California, Washington, Indiana, and Colorado's consumer protection statutes. In response, Plaintiffs cite to cases that did not address the statutes at issue or involved different injuries than those alleged by those Plaintiffs. ECF No. 72, PageID.1533-34. For example, *In re Target Corp. Data Security Breach Litigation*, 66 F. Supp. 3d 1154 (D. Minn. 2014) involved allegations of "economic injury, in the form of unreimbursed late fees, new card

fees, and other charges." *Id.* at 1162.[22] In contrast, the six Plaintiffs identified above have not alleged any unreimbursed fees or charges or any other economic injury. Nor have Plaintiffs adequately alleged that they paid any money "for the security services which they claim were not provided," which dooms their benefit-of-the-bargain theory of damages. *Gardiner v. Walmart Inc.*, 2021 WL 2520103, at *6 (N.D. Cal. Mar. 5, 2021); *see also* ECF No. 58, PageID.708.[23]

Second, all Plaintiffs, including those that allege misuse of their PII, fail to sufficiently connect their purported injuries to the Cyber Incident or any alleged deceptive act committed by Flagstar. *See supra* Section I.A.

Third, Plaintiffs fail to allege fraud with particularity. Plaintiffs are wrong that their statutory claims—which are premised on purported misrepresentations and omissions[24]—are not subject to Rule 9(b)'s heightened pleading standard. *See*,

[22] *See also Williams v. Foremost Ins. Co. Grand Rapids Mich.*, 2018 WL 1907523, at *5 (allegation that plaintiff took out loan and paid interest and fees as a result of defendant's refusal to pay insurance proceeds may be compensable under WCPA).

[23] With respect to the UCL claim, Plaintiffs claim that they have alleged that they have "no adequate remedy at law." ECF No. 72, PageID.1535, but Plaintiffs have "not demonstrated that the potential harm caused by [Flagstar's] failure to protect its customers could not be remedied by monetary damages." *Gardiner*, 2021 WL 2520103, at *7.

[24] *See, e.g.*, Compl. ¶¶ 217(d)-(g), 245(d)-(g). To the extent Plaintiffs are withdrawing their allegations of misrepresentations, omissions, and fraud under these statutes and proceeding on purportedly unfair or unconscionable acts, those claims still fail because Plaintiffs do not adequately allege that Flagstar committed any unfair or unconscionable conduct. ECF No. 58, PageID.734.

e.g., *Goodwin v. CitiMortgage, Inc.*, 2013 WL 4499003, at *5 (W.D. Mich. Aug. 19, 2013). Plaintiffs are also wrong that their claims meet Rule 9(b)'s heightened pleading standard. ECF No. 72, PageID.1532. While Plaintiffs rely on *In re Experian Data Breach Litigation* to demonstrate they have pled misrepresentations with particularity, ECF No. 72, PageID.1532, the court in that case held that what Plaintiffs describe as "essentially identical claims" to their own did *not* meet Rule 9(b)'s particularity requirement. 2016 WL 7973595, at *9 (C.D. Cal. Dec. 29, 2016). Plaintiffs are also wrong that they have adequately pled reliance by stating that they would have acted differently if they had known the truth about Flagstar's security practices. ECF No. 72, PageID.1533. The only purported misrepresentations alleged by Plaintiffs are statements in Flagstar's privacy policies that were in effect at the time of or after the Cyber Incident. Plaintiffs do not allege any misrepresentations prior to or at the time Plaintiffs became customers of Flagstar. Finally, while an omission-based claim may be cognizable under the UCL, it is not under the MCPA, CLRA, and IDSCA. *See* ECF No. 58, PageID.734. Plaintiffs cite no authority to the contrary.

Dated: April 5, 2024

Respectfully submitted,

/s/ Marcella Lape
Marcella Lape

CERTIFICATE OF SERVICE

I hereby certify that on April 5, 2024, I caused a true and correct copy of the foregoing Reply Brief in Support of Defendants' Motion to Dismiss the Consolidated Class Action Complaint to be filed electronically with the Clerk of the Court using the CM/ECF system, which will automatically send notice of such filing to all counsel of record.

/s/ Marcella Lape
Marcella Lape